



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/664,069	09/16/2003	Cheh Goh	B-5236 621255-8	3247

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
12/31/2007	PAPER

7590 12/31/2007  
HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

AK

<b>Office Action Summary</b>	<b>Application No.</b> 10/664,069	<b>Applicant(s)</b> GOH ET AL.	
	<b>Examiner</b> Beemnet W. Dada	<b>Art Unit</b> 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 October 2004.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4, 11-18, 25-28, 30, 31 and 35-38 is/are rejected.
- 7) ☒ Claim(s) 5-10, 19-24, 29, 32-34 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### DETAILED ACTION

1. This office action is in reply to an amendment filed on 10/09/07. Claims 1-38 are pending.

### ***Response to Arguments***

2. Applicant's arguments filed 10/09/07, with respect to claim rejections by Pienado (US 2002/0013772 A1) have been fully considered but they are not persuasive. Applicant argues that, in Pienado, no indication could be found that the DRM content is encrypted other than under the key KD - the subsequent encryption of the key KD itself under PU-BB-PD is clearly not relevant. Applicant further argued that, Pienado fails to teach the recitation that "the second computing entity being arranged to generate this decryption in dependence on the encryption key string and private data related to said public data". Examiner disagrees.
3. It is understood by the examiner in view of the specification that 'a computing entity arranged to encrypt a data set based on encryption parameters, that comprises: public data of a third party and an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set' as recited in claim 1 is equivalent to 'encryption of content with a first encryption key and encrypting the first encryption key with a second encryption key, wherein the first encryption key defines a policy for allowing the output of the content' (see specification page 7, line 9 - page 9, line 10). Furthermore, 'generating a decryption key in dependence on the encryption key string and private data related to said public data' is understood by the examine to be equivalent to 'decryption of the content key using a private key that is related to the public key that was used to encrypt the content key'. Therefore, examiner would point out that, Pienado teaches a first computing entity arranged to

encrypt a first data set (i.e., content) based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key, KD) comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium (i.e., license/sub-license), the first computing entity being further arranged to output the encrypted first data set for the output device (i.e., content being encrypted according to content key, content key being encrypted according to PU-BB-PD/black box public key, and delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292), and a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data (i.e., the portable device/black box decrypting the content key by using private key, PR-BB-PD, that is related to the public key, see paragraphs 0278, 0284-0292). Examiner would further point out that the art on record teaches the claim limitations and therefore, the rejection is respectfully maintained.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4, 11-18, 25-28, 30, 31 and 35-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Peinado US 2002/0013772 A1.

6. As per claims 1 and 11-13, Peinado teaches a system comprising:

an output device for outputting data onto a removable storage medium (i.e., figure 13, portable device) ;

a first computing entity arranged to encrypt a first data set (i.e., content) based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key, KD) comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium (i.e., license/sub-license), the first computing entity being further arranged to output the encrypted first data set for the output device (i.e., content being encrypted according to content key, content key being encrypted according to PU-BB-PD/black box public key, and delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292); and

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data (i.e., the portable device/black box decrypting the content key by using private key, PR-BB-PD, that is related to the public key, see paragraphs 0278, 0284-0292);

the output device being arranged to use the decryption key in decrypting the encrypted first data set (i.e., the portable device using the content key and decrypting the content, see paragraphs 0278, 0284-0292).

7. As per claims 15, 25 and 26, Peinado teaches a data output method comprising the steps of:

(a) encrypting a first data set based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key) comprising a second data set that defines a policy (i.e., license/sub-license) for allowing the output of the first data set to a removable storage medium (i.e., content being encrypted according to content key, content key being encrypted according to PU-BB-PD/black box public key, and delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292),

(b) providing the encrypted first data set to an output device adapted to output data to a removable storage medium (i.e., delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292);

(c) at the trusted party (portable device black box) checking that said policy has been satisfied and thereafter providing the output device with a decryption key for use in decrypting the encrypted first data set, this decryption key being generated in dependence on the encryption key string and private data related to said public data (i.e., the portable device/black box decrypting the content key by using private key, PR-BB-PD, that is related to the public key, see paragraphs 0278, 0284-0292); and

(d) at the output device using the decryption key in decrypting the encrypted first data set and outputting the first data set to a removable recording medium (i.e., the portable device using the content key and decrypting the content, see paragraphs 0278, 0284-0292).

8. As per claims 28, 30, 31 and 35-37, Peinado teaches a printing system comprising:  
a printer [paragraphs 036, 0099, 0267];

a first computing entity arranged to encrypt a first data set (i.e., content) based on encryption parameters comprising public data of a trusted party (i.e., PU-BB-PD) and an encryption key string (i.e., content key, KD) comprising a second data set that defines a policy for allowing the output/printing of the first data set onto a said removable storage medium (i.e., license/sub-license), the first computing entity being further arranged to output the encrypted first data set for the output device/printing device (i.e., content being encrypted according to content key, content key being encrypted according to PU-BB-PD/black box public key, and delivering the encrypted content and sub-license to the portable device, see paragraphs 0278, 0284-0292); and

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data (i.e., the portable device/black box decrypting the content key by using private key, PR-BB-PD, that is related to the public key, see paragraphs, 0278, 0284-0292);

the output device/printer being arranged to use the decryption key in decrypting the encrypted first data set (i.e., the portable device using the content key and decrypting the content, see paragraphs 0278, 0284-0292).

9. As per claims 2 and 16, Peinado further teaches the system wherein the second computing entity is arranged to generate the decryption key only when said policy has been met [see paragraphs, 0278, 0284-0292].

10. As per claims 3 and 17, Peinado further teaches the system wherein the second computing entity is arranged to issue to the first computing entity at least one of: the second data set, the encryption key string; a derivative of the encryption key string usable by the first computing entity, in place of the encryption key string, in the encryption of said first data set [paragraphs 0278, 0284-0292].

11. As per claims 4 and 18, Peinado further teaches the system wherein the second computing entity is arranged to receive the encryption key string directly or indirectly from the first computing entity [paragraphs 0278, 0284-0292].

12. As per claims 14, 27 and 38, Peinado further teaches the system further comprising a portable device comprising the second computing entity and a first communications interface, the output device comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the output device, the communications interfaces being such that the portable device must be present at the output device for the communication between the second computing entity to take place [see figure 13].

### ***Allowable Subject Matter***

Claims 5-10, 19-24, 29 and 32-34 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

### ***Conclusion***



**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

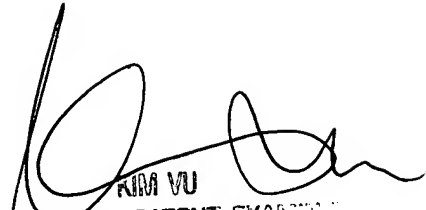
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number:  
10/664,069  
Art Unit: 2135

Page 9

Beemnet W Dada

December 22, 2007.

  
KIM VU  
UNITED STATES PATENT EXAMINER  
FEDERAL BUREAU OF INVESTIGATION